UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,124	09/25/2006	David Roxburgh	36-2015	8934

23117 7590 08/28/2008

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
VU, BAI D	

ART UNIT	PAPER NUMBER
2165	

MAIL DATE	DELIVERY MODE
08/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/594,124	ROXBURGH ET AL.	
	Examiner	Art Unit	
	Bai D. Vu	2165	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-6, 8 and 16-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-6, 8 and 16-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 May 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant has amended claims 2-6 and 8, cancelled claims 1, 7 and 9-15, and added new claims 16-18 in the amendment filed on 05/21/2008.

Claims 2-6, 8 and 16-18 are pending in this Office Action.

Response to Arguments

2. Applicant's arguments filed on 05/21/2008 with respect to claims 2-6, 8 and 16-18 have been considered but are moot in view of the new ground(s) of rejection.

Specification

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o).

Claim 18 recites “computer readable storage media” in line 1. The specification fails to explicitly provide definitions and/or limitations for “computer readable storage media”, thus insufficiently supports the claimed limitations.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. **Claims 2-6, 8 and 16** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As per **claim 16** is system claim. The system contains no hardware. Thus, the claim lacks the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are nonstatutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)

Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal,

does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

As such, claims 2-6 and 8 are rejected as incorporating the deficiencies of a claim 16 which they depend.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. **Claims 16-18** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The added limitations "when the notification means is requested so to do by any one of the services offered by the first sub-system" in claim 16 lines 13-14; "sending a request from a service wishing to set up a secure and authenticated connection to an application hosting sub-system" in claim 17 lines 9-10; and "computer readable storage media containing a program or suite of computer programs for controlling one or more

computer processors to carry out the steps of claim 17 during execution of the computer program or suite of programs" in claim 18, contains subject matter which was not described in the instant specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As such, claims 2-6 and 8 are rejected as incorporating the deficiencies of claim 16 which they depend.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. **Claims 2, 8, 16 and 17** are rejected under 35 U.S.C. 102(b) as being anticipated by Grantges, Jr. et al. (US Pat. No. 6,510,464 B1), hereinafter Grantges.

As per **claim 16**, Grantges discloses "a system comprising:

"a first sub-system and a gateway for offering services provided by the first sub-system to one or more application hosting sub-systems via the gateway;" as cited herein *FIG. 1*; and *computer system 20 is configured generally to provide access by user 18 of a client computer 22 to one of a plurality of software applications 24.sub.1,*

24.sub.2, . . . , 24.sub.3. Such access is over an insecure network 26, such as the publicly used Internet, to a private, secure network where applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 reside. Each application 24.sub.1, 24.sub.2, . . . , 24.sub.3 includes a respective web server (hereinafter "destination server") 28.sub.1, 28.sub.2, . . . , 28.sub.3, and an application program 30.sub.1, 30.sub.2, . . . , 30.sub.3. Computer system 20 includes a firewall system 32, a proxy server 34 with a plug-in 36, an application gateway 38 comprising a gateway proxy server 40 with a plug-in 42 and a gateway web server 44, and an authorization server 46 (col. 4 lines 7-19) wherein user 18 of a client computer 22 interpreted as application hosting sub-system; and web servers 28.sub.1, 28.sub.2, . . . , 28.sub.3 interpreted as first sub-systems.

"the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection from each application hosting sub-system to the gateway via a non-secure data network connection, and" as cited herein *FIGS. 1 and 2*; *proxy server 34 is disposed on the insecure public network side of firewall system 32, in a so-called Demilitarized Zone (DMZ). A DMZ is located between the insecure network 26 (e.g., the Internet) and the private network's first line of defense, for example, firewall system 32. DMZ proxy server 34 is disposed between client computer 22 and the real servers associated with the substantive applications, namely, destination servers 28.sub.1, 28.sub.2, . . . , 28.sub.3. Proxy servers in general may be characterized as providing both mapping and data caching functions. In the context of the present invention, DMZ proxy server 34 is provided principally for mapping purposes (col. 5 line 58 to col. 6 line 2)*; *application*

gateway 38 is disposed on the private network side of firewall system 32, between DMZ proxy server 34 and applications 24.sub.1, 24.sub.2, . . . , 24.sub.3. Gateway 38 includes gateway proxy server 40 and gateway web server 44 (col. 6 lines 37-40); and *gateway proxy server 40 is further configured to establish third secure connection 56 within gateway 38 with web server 44. Connection 56 may be established as described above with respect to secure connection 54. Web server 44 is configured to store various HTML files and graphics, which will be served to client computer 22. In particular, the HTML and graphic files associated with computer system 20 authentication and authorization administration are resident on application gateway server 38. More particularly, web server 44 is configured to provide an "options page" to client computer 22 when user 18 is authenticated and authorized for more than one of applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 (col. 7 lines 9-21)*.

"the gateway being logically connected to the first sub-system to enable the services provided by the first sub-system to be provided to each application hosting sub-system via a secured and authenticated connection," as cited herein *FIG. 2*; and *client computer 22 requests, by way of message 76, resources from gateway web server 44. Gateway web server 44 serves up the requested resource, namely an "options page", to client computer 22 in message 78. The "options page" presents a list of authorized applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for selection by user 18 of client computer 22. The selection of one of the applications presented on the "options page" results in a message 80 being sent to DMZ proxy server 34. Message 80 is an HTTP command (over secure connection 54, thus HTTPS) that includes a composite*

URL comprising a base URL and an appended identifier. DMZ proxy server 34 routes message 80, based on the composite URL, to gateway proxy server in a message 82. The identifier is sufficient for gateway proxy server 40 to route message 82 to the selected application 24.sub.1, 24.sub.2, . . . , 24.sub.3 (col. 9 lines 19-35).

"the gateway including notification means for notifying one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system" as cited herein *FIGS. 1 and 2*; *gateway proxy server 40 in turn passes information from the digital certificate tendered by the user of client computer 22 to authorization server 46, preferably in accordance with the LDAP protocol. Authorization server 46 returns authentication data indicative of whether the provided digital certificate successfully authenticates the user of client computer 22, as well as the identification of the applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 to which access by the user 18 has been authorized. This information is returned, in a manner to be described in greater detail below, to DMZ proxy server 34 by gateway proxy server 40 by message 74. When the user is authorized for multiple applications, the user's browser is redirected to server 44. Client computer 22 requests, by way of message 76, resources from gateway web server 44. Gateway web server 44 serves up the requested resource, namely an "options page", to client computer 22 in message 78. The "options page" presents a list of authorized applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for selection by user 18 of client computer 22. The selection of one of the applications presented on the "options page" results in a message 80 being sent to*

DMZ proxy server 34. Message 80 is an HTTP command (over secure connection 54, thus HTTPS) that includes a composite URL comprising a base URL and an appended identifier. DMZ proxy server 34 routes message 80, based on the composite URL, to gateway proxy server in a message 82. The identifier is sufficient for gateway proxy server 40 to route message 82 to the selected application 24.sub.1, 24.sub.2, . . . , 24.sub.3 (col. 9 lines 6-34); and *as described above, authorization server 46 returns authentication data to gateway proxy server 40 indicative of whether the tendered digital certificate successfully authenticated the user 18 of client computer 22, as well as an identification of applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for which access is authorized. In response thereto, gateway proxy server 40 builds authentication cookie 90, and applications list cookie 92. Authentication cookie 90 may include information such as timestamp information indicating a time of successful authentication. Applications list cookie 92 may include an identification of the particular applications for which client computer 22 is authorized. If only one application is authorized, selected application cookie 94 is built containing a description of that application. If there are a plurality of authorized applications, however, creation of the selected-application cookie 94 is deferred until after user 18 actually selects one of the applications from the "options page". The authentication cookie 90 and the application list cookie 92 are sent with message 74 to client computer 22 via DMZ proxy server 34, with a redirect to web server 44 (col. 10 lines 6-25)* wherein message 74 included information about the identification of the applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 to which access by the user 18 has been authorized interpreted as notification means.

As per **claim 17**, Grantges discloses "a method of offering services provided by a first sub-system to one or more application hosting sub-systems via a gateway, the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection from each application hosting sub-system to the gateway via a non-secure data network connection, and the gateway being logically connected to the first sub-system to enable the services provided by the first sub-system to be provided to each application hosting sub-system via a secured and authenticated connection," as cited herein *FIGS. 1 and 2*; *computer system 20 is configured generally to provide access by user 18 of a client computer 22 to one of a plurality of software applications 24.sub.1, 24.sub.2, . . . , 24.sub.3. Such access is over an insecure network 26, such as the publicly used Internet, to a private, secure network where applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 reside. Each application 24.sub.1, 24.sub.2, . . . , 24.sub.3 includes a respective web server (hereinafter "destination server") 28.sub.1, 28.sub.2, . . . , 28.sub.3, and an application program 30.sub.1, 30.sub.2, . . . , 30.sub.3. Computer system 20 includes a firewall system 32, a proxy server 34 with a plug-in 36, an application gateway 38 comprising a gateway proxy server 40 with a plug-in 42 and a gateway web server 44, and an authorization server 46 (col. 4 lines 7-19)* wherein user 18 of a client computer 22 interpreted as application hosting sub-system; and web servers 28.sub.1, 28.sub.2, . . . , 28.sub.3 interpreted as first sub-systems; *proxy server 34 is disposed on the insecure public network side of firewall system 32, in a so-called*

Demilitarized Zone (DMZ). A DMZ is located between the insecure network 26 (e.g., the Internet) and the private network's first line of defense, for example, firewall system 32. DMZ proxy server 34 is disposed between client computer 22 and the real servers associated with the substantive applications, namely, destination servers 28.sub.1, 28.sub.2, . . . , 28.sub.3. Proxy servers in general may be characterized as providing both mapping and data caching functions. In the context of the present invention, DMZ proxy server 34 is provided principally for mapping purposes (col. 5 line 58 to col. 6 line 2); *application gateway 38 is disposed on the private network side of firewall system 32, between DMZ proxy server 34 and applications 24.sub.1, 24.sub.2, . . . , 24.sub.3. Gateway 38 includes gateway proxy server 40 and gateway web server 44 (col. 6 lines 37-40)*; and *gateway proxy server 40 is further configured to establish third secure connection 56 within gateway 38 with web server 44. Connection 56 may be established as described above with respect to secure connection 54. Web server 44 is configured to store various HTML files and graphics, which will be served to client computer 22. In particular, the HTML and graphic files associated with computer system 20 authentication and authorization administration are resident on application gateway server 38. More particularly, web server 44 is configured to provide an "options page" to client computer 22 when user 18 is authenticated and authorized for more than one of applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 (col. 7 lines 9-21)* "the method comprising:"

"sending a request from a service wishing to set up a secure and authenticated connection to an application hosting sub-system that the notification means send a

notification to a respective application hosting sub-system to notify it that it should initiate a secure authenticated connection with the gateway;" as cited herein *FIGS. 1 and 2*; *gateway proxy server 40 in turn passes information from the digital certificate tendered by the user of client computer 22 to authorization server 46, preferably in accordance with the LDAP protocol. Authorization server 46 returns authentication data indicative of whether the provided digital certificate successfully authenticates the user of client computer 22, as well as the identification of the applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 to which access by the user 18 has been authorized. This information is returned, in a manner to be described in greater detail below, to DMZ proxy server 34 by gateway proxy server 40 by message 74. When the user is authorized for multiple applications, the user's browser is redirected to server 44. Client computer 22 requests, by way of message 76, resources from gateway web server 44. Gateway web server 44 serves up the requested resource, namely an "options page", to client computer 22 in message 78. The "options page" presents a list of authorized applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for selection by user 18 of client computer 22. The selection of one of the applications presented on the "options page" results in a message 80 being sent to DMZ proxy server 34. Message 80 is an HTTP command (over secure connection 54, thus HTTPS) that includes a composite URL comprising a base URL and an appended identifier. DMZ proxy server 34 routes message 80, based on the composite URL, to gateway proxy server in a message 82. The identifier is sufficient for gateway proxy server 40 to route message 82 to the selected application 24.sub.1, 24.sub.2, . . . , 24.sub.3 (col. 9 lines 6-34)*; and *as described above, authorization server*

46 returns authentication data to gateway proxy server 40 indicative of whether the tendered digital certificate successfully authenticated the user 18 of client computer 22, as well as an identification of applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for which access is authorized. In response thereto, gateway proxy server 40 builds authentication cookie 90, and applications list cookie 92. Authentication cookie 90 may include information such as timestamp information indicating a time of successful authentication. Applications list cookie 92 may include an identification of the particular applications for which client computer 22 is authorized. If only one application is authorized, selected application cookie 94 is built containing a description of that application. If there are a plurality of authorized applications, however, creation of the selected-application cookie 94 is deferred until after user 18 actually selects one of the applications from the "options page". The authentication cookie 90 and the application list cookie 92 are sent with message 74 to client computer 22 via DMZ proxy server 34, with a redirect to web server 44 (col. 10 lines 6-25) wherein message 74 included information about the identification of the applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 to which access by the user 18 has been authorized interpreted as request means.

"causing the application hosting sub-system to set up a secure and authenticated connection with the gateway in response to receipt of the notification, and communicating with the initiating service via said connection" as cited herein *FIG. 2*; and *client computer 22 requests, by way of message 76, resources from gateway web server 44. Gateway web server 44 serves up the requested resource, namely an "options page", to client computer 22 in message 78. The "options page" presents a list*

of authorized applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for selection by user 18 of client computer 22. The selection of one of the applications presented on the "options page" results in a message 80 being sent to DMZ proxy server 34. Message 80 is an HTTP command (over secure connection 54, thus HTTPS) that includes a composite URL comprising a base URL and an appended identifier. DMZ proxy server 34 routes message 80, based on the composite URL, to gateway proxy server in a message 82. The identifier is sufficient for gateway proxy server 40 to route message 82 to the selected application 24.sub.1, 24.sub.2, . . . , 24.sub.3 (col. 9 lines 19-35).

As per **claim 2**, Grantges discloses "the system according to claim 16 in which the notification takes the form of a non-executable data file" as cited *client computer 22 requests, by way of message 76, resources from gateway web server 44. Gateway web server 44 serves up the requested resource, namely an "options page", to client computer 22 in message 78. The "options page" presents a list of authorized applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for selection by user 18 of client computer 22 (col. 6 lines 36-39) interpreted as public key certificates. The selection of one of the applications presented on the "options page" results in a message 80 being sent to DMZ proxy server 34. Message 80 is an HTTP command (over secure connection 54, thus HTTPS) that includes a composite URL comprising a base URL and an appended identifier. DMZ proxy server 34 routes message 80, based on the composite URL, to gateway proxy server in a message 82. The identifier is sufficient for gateway proxy server 40 to route message 82 to the selected application 24.sub.1,*

24.sub.2, . . . , 24.sub.3 (col. 9 lines 19-34) wherein the options page in message 80 clearly encompasses claimed limitation.

As per **claim 8**, Grantges discloses "the system according to claim 16 wherein the first sub-system is a backend subsystem which provides services to the gateway and," as cited herein *FIGS. 1 and 2*; and *computer system 20 is configured generally to provide access by user 18 of a client computer 22 to one of a plurality of software applications 24.sub.1, 24.sub.2, . . . , 24.sub.3. Such access is over an insecure network 26, such as the publicly used Internet, to a private, secure network where applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 reside. Each application 24.sub.1, 24.sub.2, . . . , 24.sub.3 includes a respective web server (hereinafter "destination server") 28.sub.1, 28.sub.2, . . . , 28.sub.3, and an application program 30.sub.1, 30.sub.2, . . . , 30.sub.3. Computer system 20 includes a firewall system 32, a proxy server 34 with a plug-in 36, an application gateway 38 comprising a gateway proxy server 40 with a plug-in 42 and a gateway web server 44, and an authorization server 46 (col. 4 lines 7-19)* wherein each application 24.sub.1, 24.sub.2, . . . , 24.sub.3 includes a respective web server 28.sub.1, 28.sub.2, . . . , 28.sub.3 clearly encompasses interpreted as backend sub-system.

"wherein the server subsystem acts as a trusted intermediary between each application hosting subsystem and the backend subsystem" as cited herein *FIG. 6 shows information flow for a user in obtaining an X.509 digital certificate for use in the present invention. Each application 24.sub.1, 24.sub.2, . . . , 24.sub.3 has a respective*

trustee 134, who controls who is allowed to gain access to the application. Initially, a user 18 directs a message 136 to trustee 134, which includes information regarding the user. This communication (e.g., message 136) may be done by telephone. The trustee then provides the user with a user ID/password, with instructions to access the certificate authority 50 using the provided user ID/password. The trustee 134 then sends a message 138 to Information Security 48 that contains the information collected from the user 18, including what application(s) are being requested for remote access (col. 12 line 57 to col. 13 line 3).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 3, 6 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges in view of Gupta et al. (US Pat. No. 6,763,384 B1).

As per **claim 3**, Grantges does not explicitly disclose "the system according to claim 2 in which the notification takes the form of a simple text file containing an extensible Markup Language, XML, document". However, Gupta et al. discloses as cited herein *in order to reduce the amount of data that needs to be sent with each notification, the transmitted message need contain only the changed data, for example,*

the amount of the winning bid for an auction site. The client then dynamically generates a display incorporating the changed data for the user to view. An example of this is when data is sent in XML (eXtensible Markup Language). XML data contains only information regarding the content and structure of a message (col. 8 lines 58-66).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Gupta et al. teaching of notifying end users over a network of the occurrence of an event into Grantges system in order to notify the occurrence of an event by one or more servers to one or more client processes over a communication network (Gupta et al., col. 3 lines 13-15).

As per **claim 6**, Grantges does not explicitly disclose "the system according to claim 16 wherein a single notification server receives notifications from plural services and forwards these to plural client application hosting sub-systems". However, Gupta et al. discloses as cited herein *FIG. 3 illustrates dataflow in an embodiment where a notification server serves multiple application servers and multiple clients (col. 4 lines 56-58)*; and *FIG. 3 illustrates the flow of information that occurs when a message is generated. Whenever one of the application servers 20-24 generates an event for which notifications need to be sent to a client 114-118, a message monitor will inform the notification server 30. The notification server 30 determines the recipients for this notification, using the list of desired messages that the users have provided, together with the list of on-line clients 114-118. It then sends this notification using the server-*

initiated end-to-end message transfer mechanism to the receiving address identifier of the clients 114-118 (col. 8 lines 30-40).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Gupta et al. teaching of notifying end users over a network of the occurrence of an event into Grantges system in order to notify the occurrence of an event by one or more servers to one or more client processes over a communication network (Gupta et al., col. 3 lines 13-15).

As per **claim 18**, Grantges does not explicitly disclose "computer readable storage media containing a program or suite of computer programs for controlling one or more computer processors to carry out the steps of claim 17 during execution of the computer program or suite of programs". However, Gupta et al. discloses as cited herein *a computer program product having a computer usable medium having a computer program embodied therein, for providing notification of the occurrence of an event over a network, said computer program product including: computer program code means for registering a set of events of interest to one or more clients and, when said one or more clients are ready to receive notification, registering their respective address identifiers with a server; computer program code means for detecting the occurrence of an event; computer program code means for identifying which of said clients are interested in notification of said event and are currently active; and computer program code means for causing a real-time connection over said network to transmit said notification to each identified client (col. 4 lines 24-42)*.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Gupta et al. teaching of notifying end users over a network of the occurrence of an event into Grantges system in order to notify the occurrence of an event by one or more servers to one or more client processes over a communication network (Gupta et al., col. 3 lines 13-15).

12. **Claim 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges in view of Nishizawa et al. (US Pat. No. 6,081,906 A).

As per **claim 4**, Grantges does not explicitly disclose "the system according to claim 16 wherein the notification means is operable to run separate threads for controlling the forwarding of separate notifications to the client application". However, Nishizawa et al. discloses as cited herein *FIG. 7 is a timing chart showing multi -thread RPC processing of the event notification. The processing shown in FIG. 7 is similar to that shown in FIG. 4, except that the notification client 50 is provided with a notification N.sub.i at the conclusion of the "SendEvent" processing. Two RPC servers 20 send the first and the second RPC requests PR1 and PR2 to the notification server 40. The first and second "SendEvent" requests PR1 and PR2 arrive at the notification server 40 simultaneously, or substantially simultaneously (T1). The response thread 25 loads the first and the second "SendEvent" requests PR1 and PR2 into the queue 21 and the database 22 and immediately returns the first and the second responses R1 and R2 to the respective RPC servers 20 (T1). Processing of the first and the second RPC*

requests PR1 and PR2 then proceeds in a parallel fashion using processing threads 24.sub.1 and 24.sub.2. Because the second process request PR2 is completed in a short time (T2), for example one second, the respective notification client 50 is notified of the event without any additional delay waiting for completion of processing the first request PR1. At the conclusion of processing of the first "SendEvent" request PR1 (T3), the notification N1 is forwarded to the respective notification client 50. Thus, the delay in notifying the notification clients 50 encountered when using a single -thread notification server is also eliminated (col. 5 lines 12-35).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Nishizawa et al. teaching of implementing the multi-thread processing with queuing into Grantges system in order to achieve faster response time in sending notifications to clients.

13. **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges in view of Osterman (US Pat. No. 5,935,211 A).

As per **claim 5**, Grantges does not explicitly disclose "the system according to claim 16 wherein the notification means includes means for permitting each service provided by the first sub-system to specify the number of times which a notification is to be retried in the event of failure to deliver the notification and means for server retrying to deliver the notification up to the specified number of times in the event of failure to deliver the notification over the unsecure network". However, Osterman discloses as

cited herein *use of the time entries permits the server process to remove inactive processes from the distributed notification list. In particular, the server process may remove from the list any entry for which a predetermined time period has expired since the entry was added to the list or since the time field of the entry was updated. For example, if low frequency polling is set to occur once every 10 minutes, then the server process might remove from the list any entries that have not been updated for twenty five minutes. The server process would remove entries from the list so that server resources would not be wasted in sending notifications to client processes that are no longer connected to the server process (col. 7 lines 43-54).*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Osterman teaching of providing status information to the client processes into Grantges system in order to provide a technique that permits client processes to reduce the frequency with which they poll the server processes. This, in turn, dramatically reduces the burden on the server process imposed by such polling (Osterman, col. 2 lines 51-54).

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bai D. Vu whose telephone number is 571-270-1751. The examiner can normally be reached on Mon - Fri 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Christian Chace can be reached on 571-272-4190. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Bai D Vu/
Examiner, Art Unit 2165

/C. T. T./
Primary Examiner, Art Unit 2169
08/19/2008

/Christian P. Chace/

Supervisory Patent Examiner, Art Unit 2165